

**DRAFT**

**U.S. Government  
Application-Level Firewall  
Protection Profile  
for  
Low-Risk Environments**

**Version 1.b**

**September 1998**

**Protection Profile Title:**

U.S. Government Application-Level Firewall Protection Profile for Low-Risk Environments.

**Criteria Version:**

This Protection Profile (PP) was developed using Version 2.0 of the Common Criteria (CC) [1].

**Constraints:**

Targets of Evaluation (TOEs) developed to satisfy this Protection Profile shall conform to CC Part 2 and CC Part 3.

**Authors:**

This Protection Profile was prepared by:

Wayne Jansen, National Institute of Standards and Technology  
Jack Walsh, National Security Agency

**Acknowledgements:**

The authors would like to acknowledge Thomas Karygiannis from the National Institute of Standards and Technology, Jandria Alexander and Mario Tinto from The Aerospace Corporation, and Kris Britton from the National Security Agency.

# Table of Contents

---

Conventions and Terminology.....	v
Conventions .....	v
Terminology.....	vi
Document Organization .....	vii
Application-Level Firewall Protection Profile.....	1
PROTECTION PROFILE (PP) INTRODUCTION .....	1
PP IDENTIFICATION .....	1
PP OVERVIEW .....	1
RELATED PROTECTION PROFILES .....	1
TARGET OF EVALUATION (TOE) DESCRIPTION .....	2
TOE SECURITY ENVIRONMENT.....	3
ASSUMPTIONS.....	4
THREATS.....	5
THREATS ADDRESSED BY THE TOE .....	5
THREATS TO BE ADDRESSED BY OPERATING ENVIRONMENT.....	6
SECURITY OBJECTIVES .....	6
INFORMATION TECHNOLOGY (IT) SECURITY OBJECTIVES.....	6
NON-IT SECURITY OBJECTIVES .....	7
IT SECURITY REQUIREMENTS .....	8
TOE SECURITY REQUIREMENTS .....	8
TOE SECURITY FUNCTIONAL REQUIREMENTS.....	8
TOE SECURITY ASSURANCE REQUIREMENTS.....	22
RATIONALE.....	32
RATIONALE FOR IT SECURITY OBJECTIVES.....	32
RATIONALE FOR NON-IT SECURITY OBJECTIVES .....	34
RATIONALE FOR FUNCTIONAL REQUIREMENTS .....	34
RATIONALE FOR ASSURANCE REQUIREMENTS .....	39

RATIONALE FOR NOT SATISFYING ALL DEPENDENCIES.....	39
Appendix A	
Vulnerability List for AVA_VLA.1 .....	41
References.....	45
Acronyms.....	47

# Conventions and Terminology

## Conventions

The notation, formatting, and conventions used in this Protection Profile are largely consistent with those used in version 2 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the Protection Profile user.

The CC allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration* are defined in paragraph 2.1.4 of Part 2 of the CC. Each of these operations is used in this Protection Profile.

The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of functional requirements is denoted by **bold text**. For an example, see FMT\_SMR.1 in this Protection Profile.

The selection operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *underlined italicized text*. For an example, see FDP\_RIP.2 in this Protection Profile

The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [ assignment\_value ]. For an example, see FIA\_AFL.1 in this Protection Profile.

The iteration operation is used in order to specify a requirement more than a single time when different operations within the each iteration of the requirement must be used. Requirements that have more than one iteration have a parenthetical following the requirement title indicating which iteration of the requirement is being read. For an example, see FDP\_IFC.1 in this Protection Profile.

As a vehicle for providing a further understanding of and context for functional requirements, “Requirements Overview” sections have been selectively added to this Protection Profile. When they appear in the text, these overviews precede either a component or set of components. They provide a discussion of the relationship between functional requirements so that the Protection Profile user can see why a component or group of components was chosen and what effect it is expected to have as a group of related functions. For an example, see the Requirements Overview which precedes the ADV\_RCR.1 assurance component.

Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define “pass-fail” criteria for

a requirement. For those components where Application Notes are appropriate, the Application Notes will follow the requirement component. For an example, see the Application Note which follows FMT\_MSA.3 in this Protection Profile.

## Terminology

In the Common Criteria, many terms are defined in section 2.3 of Part 1. The following are a subset of those definitions. They are listed here to aid the user of the Protection Profile.

***User*** — Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

***Human user*** — Any person who interacts with the TOE.

***External IT entity*** — Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

***Role*** — A predefined set of rules establishing the allowed interactions between a user and the TOE.

***Identity*** — A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.

***Authentication data*** — Information used to verify the claimed identity of a user.

From the above definitions given by the CC, the following complementary terms are defined:

***Authorized Administrator*** — A role which human users may be associated with to administer the TOE.

***Authorized external IT entity*** — Any IT product or system, outside of the TOE, allowed to interact with the TOE to perform a limited number of security functions as permitted by an authorized administrator.

# **Document Organization**

Section 1 is the introductory material for the Protection Profile

Section 2 provides a general definition for application-level firewalls.

Section 3 is a discussion of the expected environment for the firewall, in particular the assumptions that must be true about aspects such as physical, personnel, and connectivity conditions. This section then defines the set of threats that are to be addressed by either the technical countermeasures implemented in the firewall's hardware and software, or through the environmental controls.

Section 4 defines the security objectives for both the firewall and the environment in which the firewall resides.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and Part 3, respectively, that must be satisfied by the firewall.

Section 6 provides a rationale to explicitly demonstrate that the IT security objectives satisfy the threats. The section then explains how the set of requirements are complete relative to the objectives; that each security objective is addressed by one or more relevant component requirements.

Appendix A provides a list of relevant vulnerabilities against which Protection Profile compliant products must be checked.

References are provided as background material for further investigation by interested users of the Protection Profile.

Acronyms are provided to facilitate comprehension of frequently used terms.





# Application-Level Firewall Protection Profile

---

## 1 PROTECTION PROFILE (PP) INTRODUCTION

---

### 1.1 PP IDENTIFICATION

- 1 Title: U.S. Government Application-Level Firewall Protection Profile for Low-Risk Environments.
- 2 Registration: <TBD>.
- 3 Keywords: information flow control, firewall, network security, proxy server, application gateway, protection profile.

### 1.2 PP OVERVIEW

- 4 This application-level firewall Protection Profile defines the basic security requirements of U.S. Government organizations handling unclassified information in a low-risk environment. Firewalls may consist of one or more devices that serve as part of an organization's overall security defense by isolating an organization's internal network from the Internet or other external networks. Firewalls pass and block information flows based on a set of screening rules defined by an authorized administrator. This Protection Profile applies to firewalls that are capable of screening network traffic at the network, transport, and application protocol levels, authenticating users who attempt to initiate information flows through the device for certain services, authenticating the authorized administrator for actions at the firewall, and auditing security-relevant events that occur.

### 1.3 RELATED PROTECTION PROFILES:

- 5 U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments [2].

## 2 TARGET OF EVALUATION (TOE) DESCRIPTION

---

- 6 The purpose of a firewall is to provide controlled and audited access to services, both from inside and outside an organization's network, by allowing, denying, and/or redirecting the flow of data through the firewall. Figure 2.1 shows a logical representation of a firewall mediating traffic, or information flows, among internal and external networks. Although there are a number of firewall architectures and technologies, firewalls basically fall into two major categories: traffic-filter and application-level firewalls. This Protection Profile specifies the minimum security requirements for TOEs composed of an application-level firewall.

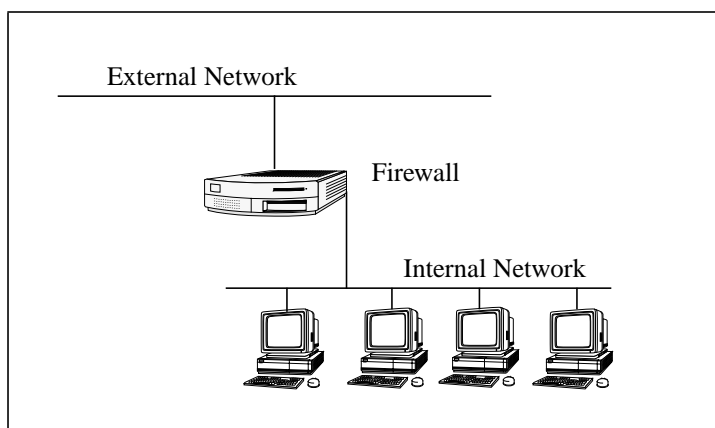


Figure 2.1 - Example of Firewall Location

- 7 The TOE mediates information flows between clients and servers located on internal and external networks governed by the TOE. TOEs may employ proxies to screen information flows. Proxy servers on the TOE, for at least the FTP and Telnet services, require authentication at the TOE by client users before requests for such services can be authorized. Thus, only valid requests are relayed by the proxy server to the actual server on either an internal or external network.
- 8 TOEs meeting this Protection Profile additionally impose traffic-filtering controls on information flows mediated by the TOE. Information flows between clients and servers according to the site's security policy rules. By default, these security policy rules deny all inbound information flows. Only an authorized administrator has the authority to change the security policy rules.
- 9 Users of the TOE consist of human users and host-like entities, called external IT entities. Human users may or may not be associated with the single role on the TOE for authorized administrators. If the information flow security policy rules permit human users who are not authorized administrators on an internal or external network to send and receive information to FTP or Telnet servers on an external or internal network, respectively, such users will have to be identified and

authenticated (using a single-use authentication mechanism) by the TOE before requests are relayed by the proxy server on the TOE to the actual server. Of the human users, only authorized administrators may access the TOE through remote means from an internal or external network. If an authorized administrator accesses the TOE remotely, and after successful identification and authentication (using a single-use authentication mechanism), a trusted channel using DES encryption with securely generated and distributed key values must be used. In addition to remote access, and after successful identification and authentication, authorized administrators may access the TOE through local means without encryption, such as through a console (that may be included as part of the TOE). Though not recommended, the human users who are not authorized administrators may identify and authenticate from a local console to use non-security functions on the TOE. The only security functions available to human users who are not authorized administrators are the controlled usage of the identification and authentication functions.

- 10 External IT entities sending information through the TOE do not have to be authenticated (using a single-use authentication mechanism), except in the case of FTP, Telnet and any other service the Security Target writer identifies. However, authorized external IT entities attempting to send information to the TOE must always be identified and authenticated (also using a single-use authentication mechanism). This subset of the external IT entities are permitted to perform a limited number of security functions as determined by an authorized administrator. A router sending routing table updates to the TOE, serves as an example of an authorized external IT entity. This router would identify itself to the TOE and then use a single-use authentication mechanism to authenticate. The TOE would then accept routing table updates from the authorized external IT entity. There are no requirements mandating authorized external IT entities.
- 11 Audit trail data is stamped with a dependable date and time when recorded. Audit events include modifications to the group of users associated with the authorized administrator role, all use of the identification and authentication mechanisms (including any attempted reuse of authentication data), all information flow control decisions made by the TOE according to the security policy rules, and the use of all security functions. If the audit trail becomes filled, then the only auditable events that may be performed are those performed by the authorized administrator. The TOE includes tools to perform searching and sorting on the collected audit trail data according to attributes of the data recorded and ranges of some of those attributes.

### **3 TOE SECURITY ENVIRONMENT**

---

- 12 Protection Profile-compliant TOEs are intended to be used either in environments in which, at most, sensitive but unclassified information is processed, or the

sensitivity level of information in both the internal and external networks is equivalent.

- 13 For all Federal agencies, including Department of Defense agencies, for the use of cryptographic modules in the protection of sensitive but unclassified information, compliance with FIPS PUB 140-1 is required<sup>1</sup>. FIPS PUB 140-1 defines security requirements for cryptographic modules. A cryptographic module is that part of a system or application that provides cryptographic services such as encryption, authentication, or electronic signature generation and verification. Products and systems compliant with this Protection Profile are expected to utilize cryptographic modules for remote administration compliant with this FIPS PUB.

### 3.1 ASSUMPTIONS

- 14 The following conditions are assumed to exist in the operational environment.

- A.PHYSEC The TOE is physically secure.
- A.LOWEXP The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
- A.GENPUR There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
- A.PUBLIC The TOE does not host public data.
- A.NOEVIL Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- A.SINGEN Information can not flow among the internal and external networks unless it passes through the TOE.
- A.DIRECT Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.

---

*1. See FIPS-PUB 140-1 for the schedule by which all cryptographic modules used by Federal agencies must meet the provisions of this standard.*

- A.SECFUN With the exception of identification and authentication, there are no security functions on the TOE accessible to human users who are not authorized administrators.
- A.NOREMO With the exception of identification and authentication, human users who are not authorized administrators can not access TOE functions remotely from the internal or external networks.
- A.REMACC Authorized administrators may access the TOE remotely from the internal and external networks.

## **3.2 THREATS**

- 15 The following threats are addressed either by the TOE or the environment.

### **3.2.1 THREATS ADDRESSED BY THE TOE**

- 16 The threats discussed below are addressed by Protection Profile-compliant TOEs. The threat agents are either human users or external IT entities not authorized to use the TOE itself. The assets that are subject to attack are the IT resources residing on the TOE itself.
- T.NOAUTH An unauthorized user may access and use security functions and/or non-security functions provided by the TOE.
- T.REPEAT A user may repeatedly try to guess authentication data.
- T.REPLAY After capturing valid user identification and authentication data, an unauthorized user may use the authentication data in the future to access functions provided by the TOE.
- T.ASPOOF A user may cause information to flow through the TOE into a connected network where the source address in the information is obviously spoofed.
- T.MEDIAT A user may send impermissible information through the TOE, including illegally formed information.

## SECURITY OBJECTIVES

- T.OLDINF A user may be able to gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.
- T.PROCOM A user may be able to view information being sent between a remotely located authorized administrator and the TOE.
- T.AUDACC A user may not be accountable for the actions that they conduct.
- T.SELPRO An unauthorized user may read, modify, or destroy TOE internal data.
- T.AUDFUL A user may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity.

### **3.2.2 THREAT TO BE ADDRESSED BY OPERATING ENVIRONMENT**

- 17 The threat possibility discussed below must be countered by procedural measures and/or administrative methods.
- T.TUSAGE The TOE may be used and administered in an insecure manner.

## **4 SECURITY OBJECTIVES**

---

### **4.1 INFORMATION TECHNOLOGY (IT) SECURITY OBJECTIVES**

- 18 The following are the IT security objectives for the TOE:
- O.IDAUTH The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions or, for certain specified services, to a connected network.
- O.SINUSE The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.
- O.MEDIAT The TOE must mediate the flow of all information from users on a connected network to users on another connected network, and must ensure that residual information from a previous information flow is not transmitted in any way.

- O.SECSTA Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources or those of any connected network.
- O.ENCRYPT The TOE must protect the confidentiality of its dialogue with an authorized administrator through encryption, if the TOE allows administration to occur remotely from a connected network.
- O.SELPRO The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
- O.AUDREC The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes.
- O.ACCOUN The TOE must provide user accountability for information flows through the TOE and for authorized administrator use of security functions.
- O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
- O.LIMEXT The TOE must provide the means for an authorized administrator to control and limit access to TOE security functions by an authorized external IT entity.

## 4.2 NON-IT SECURITY OBJECTIVES

- 19 The following are the Protection Profile non-IT security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.
- O.GUIDAN Those responsible for the TOE must ensure that the TOE is delivered, installed, administered, and operated in a manner that maintains security.
- O.ADMTRA Authorized administrators are trained as to establishment and maintenance of sound security policies and practices.

## 5 IT SECURITY REQUIREMENTS

---

### 5.1 TOE SECURITY REQUIREMENTS

20 This section provides functional and assurance requirements that must be satisfied by a Protection Profile-compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

#### 5.1.1 TOE SECURITY FUNCTIONAL REQUIREMENTS

21 The functional security requirements for this Protection Profile consist of the following components from Part 2 of the CC, summarized in the following table.

Functional Components	
FMT_SMR.1	Security roles
FIA_ATD.1	User attribute definition
FIA_UID.2	User identification before any action
FIA_UAU.1	Timing of authentication
FIA_AFL.1	Authentication failure handling
FIA_UAU.4	Single-use authentication mechanisms
FDP_IFC.1	Subset information flow control (1)
FDP_IFC.1	Subset information flow control (2)
FDP_IFF.1	Simple security attributes (1)
FDP_IFF.1	Simple security attributes (2)
FMT_MSA.3	Static attribute initialization
FDP_RIP.2	Full residual information protection
FCS_COP.1	Cryptographic operation
FPT_RVM.1	Non-bypassability of the TSP
FPT_SEP.1	TSF domain separation

**Table 5.1 - Functional Requirements**



FPT_STM.1	Reliable time stamps
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FMT_MOF.1	Management of security functions behavior

**Table 5.1 - Functional Requirements**

- 22 The following paragraphs are intended to clarify why the functional components in this Protection Profile are presented in the order outlined in Table 5.1. FMT\_SMR.1 is the first component because it defines the authorized administrator role, which appears in a number of the components that follow.
- 23 The class FIA components are listed after FMT\_SMR.1. They describe the identification and authentication policy that all users, both human users and external IT entities, must abide by before being able to use other TOE functions. Further, class FIA appears before the information flow control SFPs defined in class FDP because the second information flow SFP that is defined in FDP\_IFF.1 (2) refers back to the already defined FIA\_UAU.4 component.
- 24 The order of the class FIA components was chosen on the following basis. Since users are already defined in the Terminology section on page vi, the Protection Profile reader is introduced in component FIA\_ATD.1 to their security attributes. The next component, FIA\_UID.2, forces users to identify themselves to the TOE using the user security attributes of component FIA\_ATD.1 before further actions take place. Since authentication must follow successful identification, component FIA\_UAU.1 appears after FIA\_UID.2. Then, component FIA\_AFL.1 describes what results if the user fails to authenticate after some settable number of attempts. Lastly, component FIA\_UAU.4 discusses when single-use authentication mechanisms must be used.
- 25 There are two information flow control SFPs, and they are defined after the class FIA components in both iterations of FDP\_IFC.1. Then the policy rules which must be enforced as well as the attributes of the entities defined in FDP\_IFC.1 are written in both iterations of FDP\_IFF.1. Component FMT\_MSA.3, which FDP\_IFF.1 depends on, follows. As part of the installation and start-up of the TOE, FMT\_MSA.3 mandates a default deny policy which permits no information to flow through the TOE. FDP\_RIP.2 is listed next, ensuring that resources are cleared before being allocated to hold packets of information at the TOE.

## IT SECURITY REQUIREMENTS

- 26 Component FCS\_COP.1 is a conditional requirement. If the developer allows administration from a remote location outside the physically protected TOE, then evaluation against this Protection Profile shall require the TOE to meet this component. FCS\_COP.1 defines a cryptographic algorithm as well as the key size that must be used. The cryptographic module must be FIPS PUB 140-1 compliant for the reasons stated in Section 3.
- 27 Components dealing with the protection of trusted security functions come next. These include components FPT\_RVM.1 and FPT\_SEP.1.
- 28 Since FAU\_GEN.1 requires recording the time and date when audit events occur, it follows the FPT\_STM.1 component that alerts developers that an accurate time and date must be maintained on the TOE. The class FAU requirements follow to define the audit security functions which must be supported by the TOE. FAU\_GEN.1 is the first audit component listed because it depicts all the events that must be audited, including all the information which must be recorded in audit records. The remainder of the class FAU components ensure that the audit records can be read (component FAU\_SAR.1), searched and sorted (component FAU\_SAR.3), and protected from modification (FAU\_STG.1). Lastly, FAU\_STG.4 ensures that the TOE is capable of preventing auditable actions, not taken by an authorized administrator, from occurring in the event that the audit trail becomes full.
- 29 The last component in the profile is FMT\_MOF.1. It appears last because it lists all the functions to be provided by the TOE for use only by the authorized administrator. Almost all of these functions are based on components which precede it. Thus it is listed last.

### FMT\_SMR.1 Security roles

- 30 FMT\_SMR.1.1 - The TSF shall maintain the role [authorized administrator].
- 31 FMT\_SMR.1.2 - The TSF shall be able to associate **human** users with **the authorized administrator** role.

### FIA\_ATD.1 User attribute definition

- 32 FIA\_ATD.1.1 - The TSF shall maintain the following list of security attributes belonging to individual users:
- a) [identity;
  - b) association of a human user with the authorized administrator role;

- c) any other user security attributes to be determined by the Security Target writer(s)].

FIA\_UID.2 User identification before any action

- 33 FIA\_UID.2.1 - The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

FIA\_UAU.1 Timing of authentication

- 34 FIA\_UAU.1.1 - The TSF shall allow [identification as stated in FIA\_UID.2] on behalf of the **human user or authorized external IT entity** to be performed before the **human user or authorized external IT entity** is authenticated.

- 35 FIA\_UAU.1.2 - The TSF shall require each **human user or authorized external IT entity** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that **human user or authorized external IT entity**.

FIA\_AFL.1 Authentication failure handling

- 36 FIA\_AFL.1.1 - The TSF shall detect when [a settable, non-zero number, to be determined by the Security Target writer(s),] **of** unsuccessful authentication attempts occur related to [users not associated with the authorized administrator role attempting to authenticate from an internal or external network.]

- 37 FIA\_AFL.1.2 - When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [prevent the offending user from successfully authenticating until an authorized administrator takes some action to make authentication possible for the user in question.]

FIA\_UAU.4 Single-use authentication mechanisms

- 38 FIA\_UAU.4.1 - The TSF shall prevent reuse of authentication data related to [authentication attempts from either an internal or external network by:

- a) authorized administrators;
- b) authorized external IT entities;
- c) human users attempting to access the following services through the TOE:
  - File Transfer Protocol (FTP);
  - Telnet;
  - other services to be determined by the Security Target writer(s)].

Application Note: TOEs that do not provide capabilities for authorized administrators to access the TOE remotely from either an internal or external network (i.e., for remote administration), or for authorized external IT entities do not have to make such functionality available in order to satisfy this requirement. The intent of this requirement is not to require developers to provide these capabilities and their associated single-use authentication mechanisms. The requirement applies to those developers that do incorporate such functionality and intend for it to be evaluated. However, unlike for remote administration and authorized external IT entity functionality, TOEs must provide at least the FTP and Telnet services as well as their associated authentication mechanisms.

Requirements Overview: The TSP consists of multiple information flow control Security Function Policies (SFPs). The CC allows multiple policies to exist, each having a unique name. This is accomplished by iterating FDP\_IFC.1 for each of the two named information flow control policies. The first policy identified is called the UNAUTHENTICATED SFP. The subjects under control of this policy are external IT entities on an internal or external network sending information through the TOE to other external IT entities. The second policy identified is called the AUTHENTICATED SFP. The subjects under control of this policy are human users on an internal or external network who must be authenticated at the TOE before using the services in FIA\_UAU.4. The information flowing between subjects in both policies is traffic with attributes, defined in FDP\_IFF.1.1, including source and destination addresses. The rules that define each information flow control SFP are found in FDP\_IFF.1.2. Component FDP\_IFF.1 is iterated twice to correspond to each of the two iterations of FDP\_IFC.1.

### FDP\_IFC.1 Subset information flow control (1)

- 39 FDP\_IFC.1.1 - The TSF shall enforce the [UNAUTHENTICATED SFP] on:
- a) [subjects: unauthenticated external IT entities that send and receive information through the TOE to one another;
  - b) information: non-FTP and non-Telnet traffic [assignment: and other traffic determined by ST writers in FIA\_UAU.4.1] sent through the TOE from one subject to another;
  - c) operation: pass information].

### FDP\_IFC.1 Subset information flow control (2)

- 40 FDP\_IFC.1.1 - The TSF shall enforce the [AUTHENTICATED SFP] on:
- a) [subjects: a human user or external IT entity that sends and receives FTP and Telnet information through the TOE to one another, only after the human

user initiating the information flow has authenticated at the TOE per FIA\_UAU.4,

- b) information: FTP and Telnet traffic sent through the TOE from one subject to another;
- c) operation: initiate service and pass information].

#### FDP\_IFF.1 Simple security attributes (1)<sup>2</sup>

41 FDP\_IFF.1.1 - The TSF shall enforce the [UNAUTHENTICATED SFP] based on **at least** the following types of subject and information security attributes:

- a) [subject security attributes:
  - presumed address;
  - other subject security attributes to be determined by the Security Target writer(s);
- b) information security attributes:
  - presumed address of source subject;
  - presumed address of destination subject;
  - transport layer protocol;
  - TOE interface on which traffic arrives and departs;
  - service;
  - other information security attributes to be determined by the Security Target writer(s)].

42 FDP\_IFF.1.2 - The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

- a) [Subjects on an internal network can cause information to flow through the TOE to another connected network if:

---

*2. The complete set of functional elements of a component must be selected for inclusion in a PP. However, since the following functional elements from the FDP\_IFF.1 (1) component do not add anything significant to the PP, they have been moved here to allow for a clearer, smoother flowing presentation of FDP\_IFF.1 (1).*

*FDP\_IFF.1.3-The TSF shall enforce the [none].*

*FDP\_IFF.1.4-The TSF shall provide the following [none].*

*FDP\_IFF.1.5-The TSF shall explicitly authorize an information flow based on the following rules: [none].*

- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
  - the presumed address of the source subject, in the information, translates to an internal network address;
  - and the presumed address of the destination subject, in the information, translates to an address on the other connected network.
- b) Subjects on the external network can cause information to flow through the TOE to another connected network if:
- all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
  - the presumed address of the source subject, in the information, translates to an external network address;
  - and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

43

FDP\_IFF.1.6 - The TSF shall explicitly deny an information flow based on the following rules:

- a) [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;
- b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;
- c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;
- d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a private, reserved network;
- e) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed

address of the source subject is an external IT entity on the loopback network;

- f) The TOE shall reject malformed service requests.]

**Application Note:** The TOE can make no claim as to the real address of any source or destination subject, therefore the TOE can only suppose that these addresses are accurate. Therefore, a “presumed address” is used to identify source and destination addresses. A “service”, listed in FDP\_IFF.1.1(b), could be identified, for example, by a source port number and/or destination port number.

#### FDP\_IFF.1 Simple security attributes (2)<sup>3</sup>

44

FDP\_IFF.1.1 - The TSF shall enforce the [AUTHENTICATED SFP] based on **at least** the following types of subject and information security attributes:

- a) [subject security attributes:
  - presumed address;
  - other subject security attributes to be determined by the Security Target writer(s);
- b) information security attributes:
  - user identity;
  - presumed address of source subject;
  - presumed address of destination subject;
  - transport layer protocol;
  - TOE interface on which traffic arrives and departs;
  - service (i.e., FTP and Telnet);
  - security-relevant service command;
  - other information security attributes to be determined by the Security Target writer(s)].

---

*3. The complete set of functional elements of a component must be selected for inclusion in a PP. However, since the following functional elements from the FDP\_IFF.1 (2) component do not add anything significant to the PP, they have been moved here to allow for a clearer, smoother flowing presentation of FDP\_IFF.1 (2).*

*FDP\_IFF.1.3-The TSF shall enforce the [none].*

*FDP\_IFF.1.4-The TSF shall provide the following [none].*

*FDP\_IFF.1.5-The TSF shall explicitly authorize an information flow based on the following rules: [none].*

45

FDP\_IFF.1.2 - The TSF shall permit an information flow between a controlled subject and **another** controlled **subject** via a controlled operation if the following rules hold:

- a) [Subjects on an internal network can cause information to flow through the TOE to another connected network if:
  - the human user initiating the information flow authenticates according to FIA\_UAU.4;
  - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
  - the presumed address of the source subject, in the information, translates to an internal network address;
  - and the presumed address of the destination subject, in the information, translates to an address on the other connected network.
- b) Subjects on the external network can cause information to flow through the TOE to another connected network if:
  - the human user initiating the information flow authenticates according to FIA\_UAU.4;
  - all the information security attribute values are unambiguously permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator;
  - the presumed address of the source subject, in the information, translates to an external network address;
  - and the presumed address of the destination subject, in the information, translates to an address on the other connected network.]

46

FDP\_IFF.1.6 - The TSF shall explicitly deny an information flow based on the following rules:

- a) [The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network;
- b) The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network;



- c) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network;
- d) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a private, reserved network;
- e) The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network;
- f) The TOE shall reject malformed service requests.]

**Application Note:** The TOE can make no claim as to the real address of any source or destination subject, therefore the TOE can only suppose that these addresses are accurate. Therefore, a “presumed address” is used to identify source and destination addresses. A “service”, mentioned in FDP\_IFF.1.1(b), could be identified, for example, by a source port number and/or destination port number. A “service command”, listed in FDP\_IFF.1.1(b), refers to requests for action contained within the application protocol appropriate for screening by the TOE. For FTP, these service commands include DELE for destruction, RETR for retrieval, and STOR for creation and modification.

### FMT\_MSA.3 Static attribute initialization

47 FMT\_MSA.3.1 - The TSF shall enforce the [information flow control UNAUTHENTICATED SFP and AUTHENTICATED SFP,] to provide *restrictive* default values for **information flow** security attributes that are used to enforce the SFP.

48 FMT\_MSA.3.2 - The TSF shall allow [an authorized administrator] to specify alternative initial values to override the default values when an object or information is created.

**Application Note:** The default values for the information flow control security attributes appearing in FDP\_IFF.1 (1) and FDP\_IFF.1 (2) are intended to be restrictive in the sense that both inbound and outbound information is denied by the TOE until the default values are modified by an authorized administrator.

### FDP\_RIP.2 Full residual information protection

49 FDP\_RIP.2.1 - The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* all **subjects**.

## IT SECURITY REQUIREMENTS

Application Note: If, for example, the TOE pads information with bits in order to properly prepare the information before sending it out an interface, these bits would be considered a “resource”. The intent of the requirement is that these bits shall not contain the remains of information that had previously passed through the TOE. The requirement is met by overwriting or clearing resources before making them available for use.

### FCS\_COP.1 Cryptographic operation

50 FCS\_COP.1.1 - The TSF shall perform [encryption of remote authorized administrator sessions] in accordance with a specified cryptographic algorithm:

- [Data Encryption Standard (DES) as specified in FIPS PUB 46-2 [3] and implementing any mode of operation specified in FIPS PUB 81 [4]]

51 and cryptographic key sizes [that are 64 binary digits in length] that meet the following: [FIPS PUB 46-2 [3] and FIPS PUB 81 [4]].

Application Note: This requirement is applicable only if the TOE includes the capability for the authorized administrator to perform security functions remotely from a connected network. In this case, DES encryption must protect the communications between the authorized administrator and the TOE, and the associated cryptographic module(s) must comply at a minimum with FIPS PUB 140-1 Level 1.

### FPT\_RVM.1 Non-bypassability of the TSP

52 FPT\_RVM.1.1 - The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

### FPT\_SEP.1 TSF domain separation

53 FPT\_SEP.1.1 - The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

54 FPT\_SEP.1.2 - The TSF shall enforce separation between the security domains of subjects in the TSC.

### FPT\_STM.1 Reliable time stamps

55 FPT\_STM.1.1 - The TSF shall be able to provide reliable time stamps for its own use.

**Application Note:** The word “reliable” in the above requirement means that the order of the occurrence of auditable events is preserved. Reliable time stamps, which include both date and time, are especially important for TOEs comprised of greater than one component.

#### FAU\_GEN.1 Audit data generation

56 FAU\_GEN.1.1 - The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions;
- b) All **relevant** auditable events for the *minimal or basic* level of audit **specified in Table 5.2**; and
- c) [the event in Table 5.2 listed at the “extended” level].

57 FAU\_GEN.1.2 - The TSF shall record within each audit record at least the following information:

- a) Date and time of the event, type of event, subjects’ identities, outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column four of Table 5.2].

Functional Component	Level	Auditable Event	Additional Audit Record Contents
FMT_SMR.1	minimal	Modifications to the group of users that are part of <b>the authorized administrator</b> role.	User identity being associated or disassociated with the authorized administrator role.
FIA_UID.2	basic	All use of the user identification mechanism, including the user identity provided.	
FIA_UAU.1	basic	Any use of the authentication mechanism.	

**Table 5.2 - Auditable Events**

## IT SECURITY REQUIREMENTS

Functional Component	Level	Auditable Event	Additional Audit Record Contents
FIA_AFL.1	minimal	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g., disabling of a terminal) taken and the subsequent <b>restoration by the authorized administrator of the users capability to authenticate.</b>	
FDP_IFF.1 (1)	basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FDP_IFF.1 (2)	basic	All decisions on requests for information flow.	The presumed addresses of the source and destination subject as well as the human user identity initiating the information flow.
FCS_COP.1	minimal	Success and failure, and the type of cryptographic operation	
FPT_STM.1	minimal	Changes to the time.	
FMT_MOF.1	extended	Use of the functions listed in this requirement.	User identity associated with the authorized administrator using the function.

**Table 5.2 - Auditable Events**

### FAU\_SAR.1 Audit review

58 FAU\_SAR.1.1 - The TSF shall provide [an authorized administrator] with the capability to read [all audit trail data] from the audit records.

59 FAU\_SAR.1.2 - The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

### FAU\_SAR.3 Selectable audit review

60 FAU\_SAR.3.1 - The TSF shall provide the ability to perform searches and sorting of audit data based on:

- a) [user identity;
- b) presumed subject address;
- c) ranges of dates;

- d) ranges of times;
- e) ranges of addresses].

**Application Note:** The Security Target writer(s) is expected to describe, as part of their “Security requirements rationale” section, the capabilities of the tool(s) used by the TOE to perform these searches and sorts.

#### FAU\_STG.1 Protected audit trail storage

61 FAU\_STG.1.1 - The TSF shall protect the stored audit records from unauthorized deletion.

62 FAU\_STG.1.2 - The TSF shall be able to *prevent* modifications to the audit records.

#### FAU\_STG.4 Prevention of audit data loss

63 FAU\_STG.4.1 - The TSF shall *prevent auditable events, except those taken by the authorized administrator* and [shall limit the number of audit records lost ] if the audit trail is full.

**Application Note:** The Security Target writer(s) is expected to provide, as part of their “Security requirements rationale” section, an analysis of the maximum amount of audit data that can be expected to be lost in the event of audit storage failure, exhaustion, and/or attack.

#### FMT\_MOF.1 Management of security functions behavior

64 FMT\_MOF.1.1 - The TSF shall **provide and** restrict the ability to *perform* the functions:

- a) [start-up and shutdown;
- b) create, delete, modify, and view information flow security policy rules that permit or deny information flows;
- c) create, delete, modify, and view user attribute values defined in FIA\_ATD.1;
- d) enable and disable single-use authentication mechanisms in FIA\_UAU.4;
- e) modify and set the threshold for the number of permitted authentication attempt failures;

## IT SECURITY REQUIREMENTS

- f) restore authentication capabilities for users that have met or exceeded the threshold for permitted authentication attempt failures;
- g) enable and disable external IT entities from communicating with the TOE (if the TOE supports external IT entities);
- h) modify and set the time and date;
- i) archive, create, delete, and empty the audit trail;
- j) backup of user attribute values, information flow security policy rules, and audit trail data, where the backup capability shall be supported by automated tools;
- k) recover to the state following the last backup;
- l) additionally, if the TSF supports remote administration from either an internal or external network:
  - enable and disable remote administration from internal and external networks;
  - restrict addresses from which remote administration can be performed;
- m) other security-relevant administrative functions to be determined by the Security Target writer(s)].

65 to [an authorized administrator].

### 5.1.2 TOE SECURITY ASSURANCE REQUIREMENTS

66 The assurance security requirements for this Protection Profile, taken from Part 3 of the CC, compose EAL2. These assurance components are summarized in the following table.

Assurance Class	Assurance Components	
Configuration management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures

**Table 5.3 - Assurance Requirements: EAL2**

Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

**Table 5.3 - Assurance Requirements: EAL2****ACM\_CAP.2 Configuration items**

Developer action elements:

67 ACM\_CAP.2.1D- The developer shall provide a reference for the TOE.

68 ACM\_CAP.2.2D- The developer shall use a CM system.

69 ACM\_CAP.2.3D- The developer shall provide CM documentation.

Content and presentation of evidence elements:

70 ACM\_CAP.2.1C- The reference for the TOE shall be unique to each version of the TOE.

71 ACM\_CAP.2.2C- The TOE shall be labelled with its reference.

72 ACM\_CAP.2.3C- The CM documentation shall include a configuration list.

73 ACM\_CAP.2.4C- The configuration list shall describe the configuration items that comprise the TOE.

74 ACM\_CAP.2.5C- The CM documentation shall describe the method used to uniquely identify the configuration items.

## IT SECURITY REQUIREMENTS

75 ACM\_CAP.2.6C- The CM system shall uniquely identify all configuration items.

Evaluator action elements:

76 ACM\_CAP.2.1E- The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### ADO\_DEL.1 Delivery procedures

Developer action elements:

77 ADO\_DEL.1.1D- The developer shall document procedures for delivery of the TOE or parts of it to the user.

78 ADO\_DEL.1.2D- The developer shall use the delivery procedures.

Content and presentation of evidence elements:

79 ADO\_DEL.1.1C- The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

Evaluator action elements:

80 ADO\_DEL.1.1E- The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### ADO\_IGS.1 Installation, generation, and start-up procedures

Developer action elements:

81 ADO\_IGS.1.1D - The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

82 ADO\_IGS.1.1C - The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

83 ADO\_IGS.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.



84 ADO\_IGS.1.2E - The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

ADV\_FSP.1 Informal functional specification

Developer action elements:

85 ADV\_FSP.1.1D - The developer shall provide a functional specification.

Content and presentation of evidence elements:

86 ADV\_FSP.1.1C - The functional specification shall describe the TSF and its external interfaces using an informal style.

87 ADV\_FSP.1.2C - The functional specification shall be internally consistent.

88 ADV\_FSP.1.3C - The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

89 ADV\_FSP.1.4C - The functional specification shall completely represent the TSF.

Evaluator action elements:

90 ADV\_FSP.1.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

91 ADV\_FSP.1.2E - The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

Application Note: This requirement can potentially be met by a combination of documents provided by the developer, including the Security Target and external interface specification.

ADV\_HLD.1 Descriptive high-level design

Developer action elements:

92 ADV\_HLD.1.1D- The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

- 93        ADV\_HLD.1.1C-    The presentation of the high-level design shall be informal.
- 94        ADV\_HLD.1.2C-    The high-level design shall be internally consistent.
- 95        ADV\_HLD.1.3C-    The high-level design shall describe the structure of the TSF in terms of subsystems.
- 96        ADV\_HLD.1.4C-    The high-level design shall describe the security functionality provided by each subsystem of the TSF.
- 97        ADV\_HLD.1.5C-    The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
- 98        ADV\_HLD.1.6C-    The high-level design shall identify all interfaces to the subsystems of the TSF.
- 99        ADV\_HLD.1.7C-    The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

- 100       ADV\_HLD.1.1E-    The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- 101       ADV\_HLD.1.2E-    The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

**Requirements Overview:** ADV\_RCR.1 ensures that there is consistency between each level of design decomposition for the TOE. Each higher level of design decomposition (the higher the level of design decomposition, the more abstract) should map to the one below it, until a level of design decomposition maps to the least abstract representation, the implementation itself. Thus, for STs derived from this Protection Profile there are four layers of abstraction (from high to low): the STs “TOE summary specification” section, the functional specification, the high-level design, and the TOE itself.<sup>4</sup>

---

*4. For related information, see section 4.2.1 in Part 1 of the CC.*

ADV\_RCR.1 Informal correspondence demonstration

Developer action elements:

- 102 ADV\_RCR.1.1D- The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

- 103 ADV\_RCR.1.1C- For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

- 104 ADV\_RCR.1.1E- The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: The intent of this requirement is for the vendor to provide, and the evaluator to confirm, that there exists accurate, consistent, and clear mappings between each level of design decomposition. Thus there can be no TOE security functions defined at a lower layer of abstraction absent from a higher level of abstraction and vice versa.

AGD\_ADM.1 Administrator guidance

Developer action elements:

- 105 AGD\_ADM.1.1D- The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

- 106 AGD\_ADM.1.1C- The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

- 107 AGD\_ADM.1.2C- The administrator guidance shall describe how to administer the TOE in a secure manner.

- 108 AGD\_ADM.1.3C- The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

## IT SECURITY REQUIREMENTS

- 109 AGD\_ADM.1.4C- The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.
- 110 AGD\_ADM.1.5C- The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
- 111 AGD\_ADM.1.6C- The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
- 112 AGD\_ADM.1.7C- The administrator guidance shall be consistent with all other documentation supplied for evaluation.
- 113 AGD\_ADM.1.8C- The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

Evaluator action elements:

- 114 AGD\_ADM.1.1E- The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### AGD\_USR.1 User guidance

Developer action elements:

- 115 AGD\_USR.1.1D- The developer shall provide user guidance.

Content and presentation of evidence elements:

- 116 AGD\_USR.1.1C- The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
- 117 AGD\_USR.1.2C- The user guidance shall describe the use of user-accessible security functions provided by the TOE.
- 118 AGD\_USR.1.3C- The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
- 119 AGD\_USR.1.4C- The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

120 AGD\_USR.1.5C- The user guidance shall be consistent with all other documentation supplied for evaluation.

121 AGD\_USR.1.6C- The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

Evaluator action elements:

122 AGD\_USR.1.1E- The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Application Note: This assurance component exists at a minimum to describe the identification and authentication security functions used by human users who are not authorized administrators on an internal or external network (i.e., human users not associated with the authorized administrator role attempting to access services listed in FIA\_UAU.4). Additionally, if authorized external IT entities and/or human users who are not authorized administrators are permitted on the TOE, it is intended that functions and interfaces for these users be described. If the developer permits human users who are not authorized administrators on the TOE, AGD\_USR.1.2C is not intended to permit security functions or interfaces to exist for such users beyond those security functions described in the CC class FIA functional components in section 5.1.1. If the developer does not permit human users who are not authorized administrators on the TOE, AGD\_USR.1.2C only applies if authorized external IT entities are permitted.

ATE\_COV.1 Evidence of coverage

Developer action elements:

123 ATE\_COV.1.1D- The developer shall provide evidence of the test coverage.

Content and presentation of evidence elements:

124 ATE\_COV.1.1C- The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

Evaluator action elements:

125 ATE\_COV.1.1E- The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

## IT SECURITY REQUIREMENTS

### ATE\_FUN.1 Functional testing

Developer action elements:

126 ATE\_FUN.1.1D- The developer shall test the TSF and document the results.

127 ATE\_FUN.1.2D- The developer shall provide test documentation.

Content and presentation of evidence elements:

128 ATE\_FUN.1.1C- The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

129 ATE\_FUN.1.2C- The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

130 ATE\_FUN.1.3C- The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

131 ATE\_FUN.1.4C- The expected test results shall show the anticipated outputs from a successful execution of the tests.

132 ATE\_FUN.1.5C- The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

Evaluator action elements:

133 ATE\_FUN.1.1E- The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

### ATE\_IND.2 Independent testing - sample

Developer action elements:

134 ATE\_IND.2.1D - The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

135 ATE\_IND.2.1C - The TOE shall be suitable for testing.

136 ATE\_IND.2.2C - The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

- 137 ATE\_IND.2.1E - The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- 138 ATE\_IND.2.2E - The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.
- 139 ATE\_IND.2.3E - The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

AVA\_SOF.1 Strength of TOE security function evaluation<sup>5</sup>

Developer action elements:

- 140 AVA\_SOF.1.1D- The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

- 141 AVA\_SOF.1.1C- For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
- 142 AVA\_SOF.1.2C- For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

- 143 AVA\_SOF.1.1E- The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
- 144 AVA\_SOF.1.2E- The evaluator shall confirm that the strength claims are correct.

**Application Note:** Strength levels or strength of function metrics are defined in this application note as follows. Strength of function shall be demonstrated for the mechanism used by the TOE to meet FIA\_UAU.1 in that the probability that authentication data can be guessed is no greater than one in one million. Strength of

---

*5. This component is intended to apply strictly to those security functions that are vulnerable to an attack involving a quantitative or statistical analysis (e.g., password guessing). A short discussion of how a security mechanism may be vulnerable is provided under the "Objectives" heading for AVA\_SOF, in Part 3 of the CC.*

## RATIONALE

function shall be demonstrated for the single-use authentication mechanism(s) used to meet FIA\_UAU.4 by demonstrating compliance with the “Statistical random number generator tests” and the “Continuous random number generator test” found in section 4.11.1 of FIPS PUB 140-1 [5]. Strength of function shall be demonstrated for the cryptographic algorithm and secret generation mechanism used to meet the CC class FCS components by demonstrating compliance with the “Cryptographic algorithm test”, the “Statistical random number generator tests”, the Pair-wise consistency test (for public and private keys)”, the “Manual key entry test”, and the “Continuous random number generator test” found in section 4.11.1 of FIPS PUB 140-1 [5]. Failure to demonstrate compliance with any of these tests indicates a failure to meet the AVA\_SOF.1 requirement.

### AVA\_VLA.1 Developer vulnerability analysis

Developer action elements:

145 AVA\_VLA.1.1D- The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.

146 AVA\_VLA.1.2D- The developer shall document the disposition of obvious vulnerabilities.

Content and presentation of evidence elements:

147 AVA\_VLA.1.1C- The documentation shall show, for all identified vulnerabilities, **including those identified in Appendix A**, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

148 AVA\_VLA.1.1E- The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

149 AVA\_VLA.1.2E- The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

## 6 RATIONALE

---

### 6.1 RATIONALE FOR IT SECURITY OBJECTIVES

O.IDAUTH This security objective is necessary to counter the threat: T.NOAUTH.



- O.SINUSE This security objective is necessary to counter the threats: T.REPEAT and T.REPLAY.
- O.MEDIAT This security objective is necessary to counter the threats: T.ASPOOF, T.MEDIAT and T.OLDINF.
- O.SECSTA This security objective is necessary to counter the threats: T.NOAUTH and T.SELPRO.
- O.ENCRYP This security objective is necessary to counter the threats: T.NOAUTH and T.PROCOM.
- O.SELPRO This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL.
- O.AUDREC This security objective is necessary to counter the threat: T.AUDACC.
- O.ACCOUN This security objective is necessary to counter the threat: T.AUDACC.
- O.SECFUN This security objective is necessary to counter the threats: T.NOAUTH, T.REPLAY and T.AUDFUL.
- O.LIMEXT This security objective is necessary to counter the threat: T.NOAUTH.

	T.NOAUTH	T.REPEAT	T.REPLAY	T.ASPOOF	T.MEDIAT	T.OLDINF	T.PROCOM	T.AUDACC	T.SELPRO	T.AUDFUL
<b>O.IDAUTH</b>	X									
<b>O.SINUSE</b>		X	X							
<b>O.MEDIAT</b>				X	X	X				
<b>O.SECSTA</b>	X								X	
<b>O.ENCRYP</b>	X						X			
<b>O.SELPRO</b>									X	X

**Table 6.1 - Summary of Mappings Between Threats and IT Security Objectives**

## RATIONALE

O.AUDREC								X		
O.ACCOUN								X		
O.SECFUN	X		X							X
O.LIMEXT	X									

Table 6.1 - Summary of Mappings Between Threats and IT Security Objectives

### 6.2 RATIONALE FOR NON-IT SECURITY OBJECTIVES

O.GUIDAN This non-IT security objective is necessary to counter the threat: T.TUSAGE.

O.ADMTRA This non-IT security objective is necessary to counter the threat: T.TUSAGE.

	T.TUSAGE
O.GUIDAN	X
O.ADMTRA	X

Table 6.2 - Summary of Mappings Between Threats and Non-IT Security Objectives

### 6.3 RATIONALE FOR FUNCTIONAL REQUIREMENTS

FMT\_SMR.1 Security roles

150 Each of the CC class FMT components in this Protection Profile depend on this component. It requires the PP/ST writer to choose a role(s). This component traces back to and aids in meeting the following objective: O.SECFUN.

FIA\_ATD.1 User attribute definition

151 This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT\_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.

FIA\_UID.2 User identification before any action

152 This component ensures that before anything occurs on behalf of a user, the users identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCOUN.

FIA\_UAU.1 Timing of authentication

153 This component ensures that users are authenticated at the TOE. The TOE is permitted to pass information (aside from FTP and Telnet information) before users are authenticated. Authentication must occur whether the user is a human user or not and whether or not the user is an authorized administrator. If the authorized administrator was not always required to authenticate, there would be no means by which to audit any of their actions. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.

FIA\_AFL.1 Authentication failure handling

154 This component ensures that human users who are not authorized administrators can not endlessly attempt to authenticate. After some number of failures that the ST writer decides, that must not be zero, the user becomes unable from that point on in attempts to authenticate. This goes on until an authorized administrator makes authentication possible again for that user. This component traces back to and aids in meeting the following objective: O.SELPRO.

FIA\_UAU.4 Single-use authentication mechanisms

155 This component was chosen to ensure that some one-time authentication mechanism is used in all attempts to authenticate at the TOE from an internal or external network. This component traces back to and aids in meeting the following objective: O.SINUSE.

FDP\_IFC.1 Subset information flow control (1)

156 This component identifies the entities involved in the UNAUTHENTICATED information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.MEDIAT.

FDP\_IFC.1 Subset information flow control (2)

157 This component identifies the entities involved in the AUTHENTICATED information flow control SFP (i.e., users of the services FTP or Telnet sending

## RATIONALE

information to servers and vice versa). The users of these services must be authenticated at the TOE. This component traces back to and aids in meeting the following objective: O.MEDIAT.

### FDP\_IFF.1 Simple security attributes (1)

158 This component identifies the attributes of the users sending and receiving the information in the UNAUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

### FDP\_IFF.1 Simple security attributes (2)

159 This component identifies the attributes of the users sending and receiving the information in the AUTHENTICAED SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.

### FMT\_MSA.3 Static attribute initialization

160 This component ensures that there is a default deny policy for the information flow control security rules. This component traces back to and aids in meeting the following objectives: O.MEDIAT, O.SECSTA and O.SECFUN.

### FDP\_RIP.2 Full residual information protection

161 This component ensures that neither information that had flown through the TOE nor any TOE internal data are used when padding is used by the TOE for information flows. This component traces back to and aids in meeting the following objective: O.MEDIAT.

### FCS\_COP.1 Cryptographic operation

162 This component ensures that if the TOE does support authorized administrators to communicate with the TOE remotely from an internal or external network that DES is used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP.

FPT\_RVM.1 Non-bypassability of the TSP

163 This component ensures that the TSF are always invoked. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT\_SEP.1 TSF domain separation

164 This component ensures that the TSF have a domain of execution that is separate and that cannot be violated by unauthorized users. This component traces back to and aids in meeting the following objective: O.SELPRO.

FPT\_STM.1 Reliable time stamps

165 FAU\_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU\_GEN.1 Audit data generation

166 This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.

FAU\_SAR.1 Audit review

167 This component ensures that the audit trail is understandable. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU\_SAR.3 Selectable audit review

168 This component ensures that a variety of searches and sorts can be performed on the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.

FAU\_STG.1 Protected audit trail storage

169 This component is chosen to ensure that the audit trail is protected from tampering. Only the authorized administrator is permitted to do anything to the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

## RATIONALE

### FAU\_STG.4 Prevention of audit data loss

170 This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU\_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.

### FMT\_MOF.1 Management of security functions behavior

171 This component was chosen and modified to some extent via permitted CC operations in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objectives: O.SECSTA, O.SECFUN and O.LIMEXT.

	O.IDAUTH	O.SINUSE	O.MEDIAT	O.SECSTA	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.LIMEXT
FMT_SMR.1									X	
FIA_ATD.1	X	X								
FIA_UID.2	X							X		
FIA_UAU.1	X	X								
FIA_AFL.1						X				
FIA_UAU.4		X								
FDP_IFC.1 (1)			X							
FDP_IFC.1 (2)			X							
FDP_IFF.1 (1)			X							
FDP_IFF.1 (2)			X							
FMT_MSA.3			X	X					X	
FDP_RIP.2			X							

**Table 6.3 - Summary of Mappings Between TOE Security Functions and IT Security Objectives**

FCS_COP.1					X					
FPT_RVM.1						X				
FPT_SEP.1						X				
FPT_STM.1							X			
FAU_GEN.1							X	X		
FAU_SAR.1							X			
FAU_SAR.3							X			
FAU_STG.1						X			X	
FAU_STG.4						X			X	
FMT_MOF.1				X					X	X

**Table 6.3 - Summary of Mappings Between TOE Security Functions and IT Security Objectives**

## 6.4 RATIONALE FOR ASSURANCE REQUIREMENTS

172 EAL2 was chosen to provide a low to moderate level of independently assured security in the absence of ready availability of the complete development record from the vendor. As such, minimal additional tasks are imposed upon the vendor to the extent that if the vendor applies reasonable standards of care to the development, evaluation may be feasible without vendor involvement other than support for functional testing and vulnerability testing verification. The chosen assurance level is consistent with the postulated threat environment. Specifically, that the threat of malicious attacks is not greater than moderate, and the product will have undergone a search for obvious flaws.

## 6.5 RATIONALE FOR NOT SATISFYING ALL DEPENDENCIES

173 Functional component FMT\_MSA.3 depends on functional component FMT\_MSA.1 Management of security attributes. In an effort to place all the management requirements in a central place, FMT\_MOF.1 was used. Therefore FMT\_MOF.1 more than adequately satisfies the concerns of leaving FMT\_MSA.1 out of this Protection Profile.

174 Functional component FCS\_COP.1 depends on the following functional components: FCS\_CKM.1 Cryptographic key generation, FCS\_CKM.4 Cryptographic key destruction and FMT\_MSA.2 Secure Security Attributes. Cryptographic modules must be FIPS PUB 140-1 compliant. If the cryptographic

## **RATIONALE**

module is indeed compliant with this FIPS PUB, then the dependencies of key generation, key destruction and secure key values will have been satisfied in becoming FIPS PUB 140-1 compliant. For more information, refer to sections 4.8.1 and 4.8.5 of FIPS PUB 140-1.



## **Appendix A**

### **Vulnerability List for AVA\_VLA.1**

This appendix addresses service or application-related vulnerabilities. If the service described in one of the following vulnerabilities is not supported by the TOE, then the vulnerability is not applicable. The TOE shall also be subject to a search for obvious operating system and platform vulnerabilities.

#### **FTP daemon vulnerabilities**

Description:

In certain versions of the FTP daemon, a vulnerability exists allowing local and remote users to gain root privileges. This is accomplished through different means for distinct version such as through the signal handling routine increasing process privileges or through exploiting the SITE EXEC command.

See the relevant CERT advisory summaries including, CA-97:16, CA-95:16, and CA-94:08.

#### **rlogin with TERM environment variable vulnerability**

Description:

If, during an rlogin attempt on certain vulnerable systems, the buffer containing the value of the TERM environment variable is overflowed, arbitrary code can be executed as root.

See the relevant CERT advisory summaries including, CA-97:06.

#### **Sendmail vulnerabilities**

Description:

Remote users may be able to execute arbitrary commands with root privileges on systems receiving mail that are running a vulnerable version of sendmail that support MIME.

A second vulnerability to certain versions of sendmail occurs when an attacker gains group permissions of another user. This is possible when mail is sent to a users .forward or :include: file which is located in a directory that is writable by the attacker.

A third vulnerability to certain versions of sendmail occurs when users other than root invoke sendmail in daemon mode, bypassing code intended to prevent this.

A fourth vulnerability to certain versions of sendmail occurs when buffer overflows lead to unauthorized users gaining root access.

A fifth vulnerability to certain versions of sendmail occurs in the case of resource starvation. A user with an account can exploit sendmail when sendmail cannot distinguish between a “resource failure” and “user id not found” error. Starving sendmail will create files owned by the “default user” which can then be used to gain access to other files owned by that user.

See the relevant CERT advisory summaries including, CA-97:05, CA-96:25, CA-96:24, CA-96:20, and CA-95:08.

## **Telnet Environment Option vulnerability**

Description:

If the system to which the Telnet connection attempt is directed is running Telnet daemons that are RFC 1408 or RFC 1572 compliant and the system supports shared object libraries then the system may be vulnerable. Both users with and without accounts on the system could become root by transferring environment variables that influence the login program called by the Telnet daemon.

See the relevant CERT advisory summaries including, CA-95:14.

## **TFTP daemon attacks**

Description:

Remote users on the Internet may access world-readable files on an internal network using an unrestricted TFTP service. Thus sensitive files could be retrieved by an adversary on the external side of the firewall.

See the relevant CERT advisory summaries including, CA-91:19 and CA-91:18.

## **Syslog Vulnerability**

The syslog(3) subroutine uses an internal buffer for building messages that are sent to the syslogd(8) daemon. This subroutine does no range checking on data stored in this buffer. It is possible to overflow the internal buffer and rewrite the subroutine call stack. It is then possible to execute arbitrary programs.

This problem is present in virtually all versions of the UNIX Operating System except the following:

- Sony's NEWS-OS 6.X
- SunOS 5.5 (Solaris 2.5)
- Linux with libc version 4.7.2 released in May, 1995

The sendmail(8) program uses the syslog(3) subroutine, and a script has been written and is being used to exploit the vulnerability.

Impact: Local and remote users can execute commands. Prior access to the system is not needed. Exploitation can lead to root access.

See the relevant CERT advisory summaries including, CA-95:13.

## **IP Spoofing attacks**

Description:

Firewalls are vulnerable to IP spoofing attacks, including TCP SYN Flooding attacks. Firewalls should have a mechanism to handle SYN Flooding attacks. Firewalls should be capable of preventing traffic from entering the protected local network when packets claim to originate from local network, broadcast network, reserved network, or loopback network addresses.

See the relevant CERT advisory summaries including, CA-96:21.

## **UDP attacks**

Description:

Tools exist to flood UDP ports with packets causing degradation in system performance and increased network congestion. Firewalls must be capable of being configured to filter all UDP services.

See the relevant CERT advisory summaries including, CA-96:01.

## **ICMP (ping) vulnerability**

Large ICMP datagrams may cause systems to crash, freeze, or reboot, resulting in a denial of service.

See the relevant CERT advisory summaries for more information including, CA-96:26.

## **IP loose source route option vulnerability**

Description:

Firewalls should be capable of rejecting packets that use the IP loose source route option. A TCP connection where the loose source route option is enabled allows an attacker to explicitly route packets through the network to a destination without following the usual routing process. A malicious attacker can pose as a host that is on the return path for this type of TCP traffic since, according to RFC 1122, the traffic must follow the reverse order of the route which it followed from source to destination.

## **RIP vulnerability**

### **Description:**

As a result of the ease with which bogus RIP packets may be injected into a network, packets can be lead away from their intended destination if the attacking host is closer to the target than the valid sending host. This occurs when routers accept RIP packets and because RIP performs no type of authentication. Firewalls should be configured to disallow routing along certain links such as intermediate links on an external network while the source and destination hosts are both on the internal network.

## **ARP vulnerability**

### **Description:**

Because any host can respond to an ARP request, a malicious host can send false ARP responses back to the sender before the true recipient receives the ARP request and responds back. Thus the sender will now be fooled into sending traffic to the malicious host in the middle rather than the proper destination host. The malicious host can either impersonate the destination host, or intercept, modify, and resend the traffic to the sending host's intended destination. Firewalls should not allow ARP requests to pass through them and should not perform proxy ARP for requests from an external network.

## **DNS vulnerabilities**

### **Description:**

A flood of DNS responses injected into the network could cause a denial of service since the DNS server may become confused.

A DNS resolver may check several different levels before checking the correct one. If a host, FOO.BAR.COM, attempts to connect to ONE.TWO, the check will be made first to ONE.TWO.BAR.COM and then to ONE.TWO.COM and finally to ONE.TWO. Thus a malicious host can impersonate a domain that the resolver would encounter before encountering the appropriate level.

If an attacker can contaminate a target's DNS responses cache before the call is made, the target can be fooled into believing that the cross-check it performs is legitimate. As a result, the attacker gains access.

## References

- [1] *Common Criteria for Information Technology Security Evaluation*, CCIB-98-026 Version 2, May 1998.
- [2] *U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments*; Version 2.0, June 1998.
- [3] Federal Information Processing Standard Publication (FIPS-PUB) 46-2, *Data Encryption Standard (DES)*, December 1993.
- [4] Federal Information Processing Standard Publication (FIPS-PUB) 81, *DES Modes of Operation*, December 1980.
- [5] Federal Information Processing Standard Publication (FIPS-PUB) 140-1, *Security Requirements for Cryptographic Modules*, dated January 11, 1994.
- [6] Building Internet Firewalls, Chapman & Zwicky, O'Reilly & Associates, Inc., November 1995.



# Acronyms

The following abbreviations from the Common Criteria are used in this Protection Profile:

<b>CC</b>	Common Criteria for Information Technology Security Evaluation
<b>EAL</b>	Evaluation Assurance Level
<b>FIPS PUB</b>	Federal Information Processing Standard Publication
<b>FTP</b>	File Transfer Protocol
<b>HTTP</b>	Hypertext Transfer Protocol
<b>IT</b>	Information Technology
<b>PP</b>	Protection Profile
<b>SFP</b>	Security Function Policy
<b>ST</b>	Security Target
<b>TOE</b>	Target of Evaluation
<b>TSC</b>	TSF Scope of Control
<b>TSF</b>	TOE Security Functions
<b>TSP</b>	TOE Security Policy

